REMARKS

This amendment is being filed in response to an Office Action mailed 10/12/2005, in which the Examiner said that claims 1-5 and 7-25 were pending but rejected. In this amendment, claim 13 is amended and new claims 26-28 are added, with various reasons for rejections being traversed below.

In claim 13, line 3, "said computer medium" is changed to "said computer readable medium" to match the antecedent basis provided in line 2 of the same claim.

Claims Rejected under 35 USC §103

In the above-mentioned Office Action, the Examiner additionally said that claims 1-7 and 11-24 were rejected under 35 USC §103(a) as being unpatentable over U.S. Pat. No. 6,832,316 to Sibert, in view of U.S. Pat. No. 6,463,537 to Tello, and further in view of U.S. Pat. No. 6,507,911 to Langford.

The Applicants' invention provides a method for preventing the reading of information stored within a first computer system, especially on a hard drive of the first computer system, in a second computer system, so that data cannot be stolen from the first computer system by removing the storage means, such as a hard disk drive, from the first computer system and reading the data. Since it is assumed that such removal of a storage device from the first computer system would occur with the first computer system turned off, the method of the invention provides encryption when the computer system is turned off and decryption when it is turned on. On the other hand, Sibert describes a method for integrating message authentication and decryption, with intermediate internal states of the decryption operation being used to detect manipulation of the encrypted data. Thus, the method of Sibert is applied to messages received by a computing

system, not to data stored within the computing system when it is turned off.

The Applicants' invention provides a method for securing a large amount of data, stored within a hard disk drive medium or on a removable computer readable medium, by encrypting a small amount of data within a data structure including information locating the various data records on the medium. This method avoids a need to encrypt and subsequently decrypt all of the data to be protected. On the other hand, the method of Sibert requires that all of the data to be protected is encrypted and subsequently decrypted, as described, for example, column 3, lines 8-12, 20-23, and column 5, lines 12-17.

Tello describes a 'personalized' computer with a unique encrypted digital signature which will not boot up or recognize any data storage or communication peripheral device without a matching 'personalized' smart card containing a complimentary encrypted digital signature, as described in the Abstract.

Langford describes a data deletion system and method providing an system invoked deletion process that modifies the desired data to be deleted.

Regarding claim 1, the Examiner further indicated that Sibert discloses a method providing security for a plurality of data records stored on a computer readable medium within a computer system, wherein said computer readable medium additionally stores a first data structure, starting at a first location within said computer readable medium, locating data records in said plurality thereof, said method being a decryption subroutine executed as said computing system is being initialized, said decryption subroutine includes determining that electrical power has been turned on in said computing system, reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure to form said first data structure (see column 6 lines 55-67) and a method for encrypting (see column 5 lines 41-67).

Regarding the above statement, the Applicants respectfully submit that, as described in claim 1 of the Applicants' invention, the first data structure must locate data records in the plurality of data records that are stored on the computer readable medium and for which security is provided by the method. On the other hand, Sibert describes, in column 6, lines 55-67, an embodiment in which decoding logic is used at system start-up to decrypt and validate *system control programs* to be operable to initialize and control the operation of the system 42. The system 42 can then be used to decrypt data. *Thus, there is no indication that the data itself is decrypted in the method of Sibert at system start-up, or that it is even available for decryption at that time. There is no indication that the system of Sibert decrypts a data structure locating data records within the data at that time or at any other time.*

Furthermore, regarding the above statement, the applicants note that the text cited by the Examiner for encrypting, column 5, lines 41-67, merely indicates that the system includes an encoding system, described in exemplary detail, for encoding messages or data and transmitting the resulting ciphertext to a recipient's system. *Thus, there is no indication that the system of Sibert decrypts a data structure locating data records.*

The Examiner additionally said that Sibert fails to disclose the encryption subroutine include receiving a request to shut down said computing system, reading said first data structure from said computer readable medium, encrypting said first data structure to produce an encrypted version of said first data structure, using a public key encryption scheme and the encryption being done to prevent reading information stored in data records when the medium is removed from the system. The Examiner then said that, however, Tello teaches performing tasks at shut down (see column 14, lines 1-41) and public key encryption (see column 8 lines 34-40) and the encryption being done to prevent

reading information stored in data records when the medium is removed from the system (see column 4 line 38 through column 5 line 14).

Regarding this statement, the Applicants respectfully note that, according to the cited text in column 14, lines 1-41, the system of Tello includes a security engine microprocessor taking over control from the motherboard CPU to secure data with a modified BIOS by hiding all data storage devices and user selected peripheral devices upon system start up and shut down. *Thus, the Examiner uses Tello only to indicate that something can happen during system shut down; there is no indication that data records locating data to be protected are being encrypted. This process of Tello does not involve any form of data encryption.* In fact, Tello teaches against the Applicant's invention, indicating that data should be protected by hiding access to storage devices instead of by encrypting data records locating data files. The other text cited in Tello, column 8, lines 34-40, suggests the use of an encryption algorithm, such as an RSA algorithm, to encrypt selected data that is to be passed to or used by another computer. *There is no reason or indication that such encryption should occur at system shut down.*

Langford is used by the Examiner to describe a method of replacing data in a computer readable medium. Adding the teachings of Langford to those of Sibert and Tello does not overcome the deficiencies described above in describing the limitations of claim 1.

For all the reasons described above, the Applicants respectfully submit that Sibert, Tello, and Langford, taken separately or in combination, fail to disclos, teach, or otherwise anticipate the requirements of claim 1 for a method, wherein

said method comprises an encryption subroutine executed as said computing system is being shut down and a decryption subroutine executed as said computing system is being initialized,

said encryption subroutine includes receiving a request to shut down said computing system, reading said first data structure from said computer readable medium, encrypting said first data structure with a public key of said computing system to produce an encrypted version of said first data structure that can only be decrypted with a private key of said computing system to prevent reading information stored in said data records with said computer readable medium removed from said computing system, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and

said decryption subroutine includes determining that electrical power has been turned on in said computing system, reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure with said private key of said computing system to form said first data structure, and writing said first data structure to said computer readable medium, starting at said first location.

For all the above reasons, the Applicants respectfully submit that claim 1 is patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 2-5, 7, 11, and 12 since these dependent claims merely add limitations to claim 1, the Applicants respectfully submit that, for reasons described above regarding claim 1, claims 2-5, 7, 11 and 12 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 13 and 19, in the above-mentioned Office Action, the Examiner said that the modified Sibert, Tello and Langford system discloses a method providing security for a plurality of data records stored on a computer

readable medium within a computing system, wherein said computer medium additionally stores a first data structure starting at a first location within said removable computer readable medium, locating data records in said plurality thereof, said method comprises an encryption subroutine executed to encrypt said first data structure and a decryption subroutine subsequently executed to decrypt an encrypted version of said first data structure, said encryption subroutine includes reading said first data structure from said computer readable medium, encrypting said first data structure within a cryptographic processor in said computing system using an encryption key to produce an encrypted version of said first data structure, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and said decryption subroutine includes reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure within said cryptographic processor in said computing system using a decryption key generated from data stored in secure storage accessed by said cryptographic processor to form said first data structure, and writing said data structure to said computer readable medium, starting at said first location (see rejection of claim 5) with the prevention of reading records when the medium is removed from the system (see Tello as applied to claim 1).

Regarding the above statement by the Examiner, the Applicant respectfully submits that, generally for reasons described above in regard to the rejection of claim 1, Sibert, Tello and Langford, taken separately or in combination, fail to describe the requirements of claims 13 and 19 for a method or a computing system wherein said encryption subroutine includes reading said first data structure from said computer readable medium, encrypting said first data structure within a cryptographic processor in said computing system using an encryption key to produce an encrypted version of said first data structure,

deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and said decryption subroutine includes reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure within said cryptographic processor.

The Applicants respectfully submit that, as described in detail above regarding the rejection of claim 1, Sibert, Tello, and Langford do not describe the encryption and subsequent decryption of a data structure describing the locations of data records on the computer readable medium being protected, with Sibert instead teaching that the entirety of the data to be protected should be encrypted and decrypted, and with Tello teaching that peripheral devices should be enabled and disabled at system start up and shut down. The Applicants further summit that these cited references fail to describe, teach, or otherwise anticipate the requirements of claim 13 for the encryption subroutine to encrypt said first data structure and for a decryption subroutine subsequently executed to decrypt said encrypted version of said first data structure, and for these encryption and decryption processes to within a cryptographic processor, *wherein said first data structure locates data records in a plurality of data records stored on a computer readable medium*.

Therefore, the Applicants respectfully submit that claims 13 and 19 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claim 14, the Applicants respectfully submit that Sibert, Tello, and Langford, taken separately or in combination, fail to describe, teach, or otherwise anticipate the requirement of claim 14 for the encryption program to be executed in response to receiving a request to shut down the computing system and for

the encryption routine to be executed in response to electrical power being turned on within the computing system. Langford does not describe encryption and decryption occurring in response to the system being shut down or turned on. Tello describes peripheral devices being disabled and enabled as the system is shut down or turned on. Sibert describes system control programs, not a data structure locating data records, being decrypted when the system is turned on. There is no indication that the control programs are encrypted when the system is turned off; they may be stored in an encrypted form whether or not the system is running.

Therefore, and additionally because claim 14 merely adds these limitations to claim 13, which is believed to be patentable for reasons described above, the Applicants respectfully submit that claim 14 is patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 15-18, the Applicants respectfully submit that, since these claims merely add limitations to claim 13, for reasons described above regarding claim 13, claims 15-18 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 20-24, the Applicants respectfully submit that, since these claims merely add limitations to claim 19, for reasons described above regarding claim 19, claims 20-24 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford.

Regarding claims 8, 9, and 25, the Examiner indicated that these claims were rejected under 33 USC §103(a) as being unpatentable over a modified Sibert, Tello, and Langford system, further in view of U.S. Pat. No. 5,544,356 to Robinson et al., with Robinson et al. teaching a boot record describing the file allocation table. Nevertheless, the Applicants respectfully submit that adding the

teachings of Robinson et al does not provide a description of the encryption and subsequent decryption of a data structure locating various data records, with such a description being missing from the disclosure of the other cited patents. Therefore, and additionally because claims 8 and 9 merely add limitations to claim 1, and further because claim 25 merely adds limitations to claim 19, the Applicants respectfully submit that claims 8, 10, and 25 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford and additionally in view of Robinson et al.

Regarding claims 8, 10, and 25, the Examiner indicated that these claims were rejected under 33 USC §103(a) as being unpatentable over a modified Sibert, Tello, and Langford system, further in view of U.S. Pat. No. 6,070,174 to Starek et al., with Starek et al. describing an array of file records in a master file table of an NTFS file, and a second data structure including metafile data in the master file table. Nevertheless, the Applicants respectfully submit that adding the teachings of Starek et al does not provide a description of the encryption and subsequent decryption of a data structure locating various data records, with such a description being missing from the disclosure of the other cited patents. Therefore, and additionally because claims 8 and 10 merely add limitations to claim 1, and further because claim 25 merely adds limitations to claim 19, the Applicants respectfully submit that claims 8, 10, and 25 are patentable under 35 USC §103(a) over Sibert in view of Tello and further in view of Langford and additionally in view of Starek et al.

Regarding claims 1-5 and 7-25, the Examiner additionally indicated that claims 1-5 and 7-25, were rejected as previously described but in view of JP2001202167A, which discloses a control method for a computer, involving the encrypting and decoding data in memory based on power on or off in the power supply. However, the Applicants respectfully submit that this Japanese patent teaches that the entire contents of the memory should be encrypted and

decrypted. Again, there is no teaching of the encryption and decryption only of a data structure describing the location of data records to be protected. *This difference between the prior art and the Applicant's invention is particularly significant, because, while JP2001202167A requires the encryption and decryption of a vast amount of data stored, for example, on a hard disk drive, the method of the Applicants' invention requires the encryption and decryption of a much smaller quantity of data, making it feasible to provide the encryption and decryption processes whenever the computing system is turned on and off. This is a key to making the process of the Applicant's invention practical.* Therefore, the Applicants respectfully submit that claims 1-5 and 7-25 are patentable under 35 USC §103(a) as described above and further in view of JP2001202167A.

Regarding claim 1, the Applicant's respectfully submit that, for reasons described in detail above, Sibert, Tello, Langford, and JP2001202167A, taken separately or in combination fail to describe the requirements of claim 1 for a method providing security for a plurality of data records stored on a computer readable medium, wherein

said computer readable medium additionally stores a first data structure, starting at a first location, *said first data structure locating data records in said plurality thereof;*

said encryption subroutine includes receiving a request to shut down said computing system, reading said first data structure from said computer readable medium, encrypting said first data structure with a public key of said computing system to produce an encrypted version of said first data structure that can only be decrypted with a private key of said computing system to prevent reading information stored in said data records with said computer readable medium removed from said computing system, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and

said decryption subroutine includes determining that electrical power has been turned on in said computing system, reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure with said private key of said computing system to form said first data structure, and writing said first data structure to said computer readable medium, starting at said first location.

Therefore, the Applicants respectfully submit that claim 1 is patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A.

Regarding claims 2-5 and 7-12, since each of these dependent claims merely adds limitations to claim 1, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A for reasons advanced above regarding claim 1.

Regarding claim 13, the Applicants respectfully submit that for reasons described in detail above, Sibert, Tello, Langford, and JP2001202167A, taken separately or in combination fail to describe the requirements of claim 13 for a method providing security for a plurality of data records stored on a computer readable medium, wherein

said computer medium additionally stores a first data structure starting at a first location within said computer readable medium, locating data records in said plurality thereof,

said method comprises *an encryption subroutine executed to encrypt said first data structure and a decryption subroutine subsequently executed to decrypt an encrypted version of said first data structure*,

said encryption subroutine includes reading *said first data structure from said computer readable medium, encrypting said first data structure within a cryptographic processor in said computing system using an encryption key to*

produce an encrypted version of said first data structure to prevent reading information stored in said data records with said computer readable medium removed said computer system, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and

said decryption subroutine includes *reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure* within said cryptographic processor in said computing system using a decryption key generated from data stored in secure storage accessed by said cryptographic processor to form said first data structure, and writing said data structure to said computer readable medium, starting at said first location.

In particular, the Applicants note that JP2001202167A teaches against encrypting and decrypting a first data structure locating data records to be protected, teaching instead that the data records to be protected should themselves by encrypted and decrypted. Therefore, the Applicants respectfully submit that claim 13 is patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A.

Regarding claims 14-18, since each of these dependent claims merely adds limitations to claim 13, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A for reasons advanced above regarding claim 1.

Regarding claim 19, the Applicants respectfully submit that for reasons described in detail above, Sibert, Tello, Langford, and JP2001202167A, taken separately or in combination fail to describe the requirements of claim 13 for a microprocessor, separate from said cryptographic processor, wherein said

microprocessor is programmed to execute a data structure encryption routine to encrypt said first data structure and to execute subsequently a data structure decryption routine to decrypt an encrypted version of said first data structure, wherein said data structure encryption routine includes causing said cryptographic processor to read said first data structure from said computer readable medium, to execute said internal encryption routine, encrypting said data structure to form said encrypted version of said first data structure, preventing reading information stored in said data records with said computer readable medium removed from said computing system and to write said encrypted version of said first data structure to nonvolatile storage, wherein said first data structure is additionally deleted from said first computer readable medium during execution of said data structure encryption subroutine, and wherein said data structure decryption subroutine includes causing said cryptographic processor to read said encrypted version of said first data structure from nonvolatile storage, to decrypt said encrypted version of said first data structure, forming said first data structure, and to write said first data structure to said computer readable medium, starting at said first location.

In particular, the Applicants note that JP2001202167A teaches against encrypting and decrypting a first data structure locating data records to be protected, teaching instead that the data records to be protected should themselves by encrypted and decrypted. Therefore, the Applicants respectfully submit that claim 13 is patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A.

Regarding claims 19-25, since each of these dependent claims merely adds limitations to claim 18, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A for reasons advanced above regarding claim 18.

New Claims

New claims 26-28 are added herein to clarify the Applicants' invention and to further differentiate this invention from the prior art cited by the Examiner.

Regarding claim 26, this new claim specifies a method, within a computing system, providing security for a plurality of data records stored with a first data structure locating data records in said plurality thereof on a computer readable medium within said computing system, wherein said method comprises:

encrypting said first data structure to form an encrypted version of said first data structure without encrypting said plurality of data records as said computing system is being shut down, and

decrypting said encrypted version of said first data structure as said computing system is being initialized.

Support for this new claim is found in the specification as originally filed on page 9, lines 27-29, on page 18, line 12, through page 19, line 17. This claim is believed to be patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A, because, of these references, only JP001202167A describes protecting data records by performing encryption and decryption at system start up and shut down, and because JP2001202167A clearly teaches encrypting the data to be protected rather than encrypting a data structure locating the data records to be protected without encrypting the data to be protected itself.

Regarding claim 27, this new claim adds to claim 26 limitations that said first data record is encrypted with a public key of said computing system and decrypted with a private key of said computing system. Support for this new claim is found in the specification as originally filed on page 15, line 26, through page 16, line 13. This claim is believed to be patentable under 35 USC §103(a) over Sibert in view of Tello, Langford, and JP2001202167A, because these

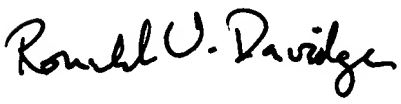
limitations are merely added to claim 26, which is believed to be patentable as described above, and additionally because none of the references describe encrypting and decrypting the a data structure specifying locations of the data records with public and private keys in this way.

Regarding claim 28, this new claim adds to claim 26, limitations that the method additionally includes writing said encrypted version of said first data structure to said computer readable medium after encrypting said first data structure; and reading said encrypted version of said first data structure from said computer readable medium before decrypting said encrypted version of said computer readable medium. This claim is believed to be patentable because such a data structure is not encrypted by Sibert, Tello, Langford, or JP2001202167A, and additionally because this claim merely adds these limitations to claim 26, which is believed to be patentable as described above.

Conclusions

The Applicants respectfully submit that the application, including claims 1-25, is now in condition for allowance, and that action is earnestly requested, with reconsideration and withdrawal of all reasons given for rejections.

Respectfully submitted,



Ronald V. Davidge
Registration No. 33,863
Telephone No. 954-344-9880

January 12, 2006